

EDWARD J. MARKEY

7TH DISTRICT, MASSACHUSETTS

ENERGY AND COMMERCE COMMITTEE

RANKING MEMBER
SUBCOMMITTEE ON
TELECOMMUNICATIONS AND
THE INTERNET

SELECT COMMITTEE ON
HOMELAND SECURITY

RESOURCES COMMITTEE

Congress of the United States
House of Representatives
Washington, DC 20515-2107

2108 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-2107
(202) 225-2836

DISTRICT OFFICES:

5 HIGH STREET, SUITE 101
MEDFORD, MA 02155
(781) 396-2900

188 CONCORD STREET, SUITE 102
FRAMINGHAM, MA 01702
(508) 875-2900
www.house.gov/markey

October 20, 2003

The Honorable Nils J. Diaz
Chairman
Nuclear Regulatory Commission
Washington, D.C. 20555

Dear Mr. Chairman:

Thank you for your reply to my letter of August 22, 2003 about the infection of the Davis-Besse nuclear plant by the "Slammer" worm computer virus. This incident raises a number of important nuclear safety and homeland security issues of concern to me both as a Member of the Energy and Commerce Committee and of the Homeland Security Committee. I appreciate your responses to the questions posed in my letter. Unfortunately, many of the responses appear to be vague, incomplete, or contradictory.

As you know, the Davis-Besse nuclear power plant operated by FirstEnergy Corp. in Oak Harbor, Ohio, was infected with the Slammer worm on January 25, 2003. As reported in August by *Security Focus News*,¹ the worm disabled two computer systems at Davis-Besse for several hours. The worm's attack was successful because plant computer engineers had failed to install a security patch to the Microsoft SQL 2000 server, even though the patch had been available for six months prior to the attack.

In order to better understand the facts and circumstances surrounding this incident, the Commission's policies, regulations and oversight activities with respect to licensee cybersecurity, and related matters, I wrote to you on August 22, 2003 with a series of questions regarding this matter. Your October 2, 2003 response to my letter, while welcome, fails to answer many of my fundamental questions and concerns about the Commission's oversight and regulatory efforts pertaining to cyber security. For this reason, I hereby request your assistance and cooperation in providing me with responses to a series of follow-up questions. I would respectfully request that such responses be provided no later than November 15, 2003.

First, the specific Davis-Besse plant infection is troubling. You state that neither of the two systems attacked by the virus "affect the safety of the facility". I find it very surprising that the infected "Safety Parameter Display System" (SPDS) and the "Plant Process Computer" (PPC) do not affect the safety of the plant. As you explain in your response, these systems "assist the operators in monitoring plant parameters".

¹ See <http://www.securityfocus.com/news/6767/>.

- Isn't it the case that SPDS was put in place as a direct result of the failure of monitoring equipment at the Three Mile Island nuclear plant during the March 28, 1979 accident?
- Isn't it also the case that SPDS relays critical plant safety parameters to the NRC Operations Center in real time?
- Isn't the monitoring of plant safety parameters and processes relevant to and necessary for the safe operation of a nuclear power plant?
- If not, why does the plant run these systems?
- What computer systems, if infected, would adversely impact the safety of the plant, and how did these escape infection from the Slammer worm?
- Could these safety-critical systems be infected by other viruses or deliberate hacking attempts? Why or why not?

You also note in your cover letter that the Davis-Besse plant was "in a safely defueled condition" at the time of the infection. This is not reassuring: future computer worms will not be polite enough to attack only defueled plants.

- What would the safety consequences of the Slammer infection have been if the plant had been fueled and operational?
- What impact would the infection have had on the ability of the licensee to monitor the plant's operation and properly respond to any problem?
- Has the NRC staff or the licensee undertaken a worst-case analysis of the impact of having these systems malfunctioning or inoperative when the reactor was operating? If so, what were the findings and recommendations of this analysis? If not, why not?
- The NRC's Information Notice 2003-14 says that the worm was removed by shutting down the MS SQL 2000 server. Would this shutdown have been possible during standard plant operation without either negative safety consequences or shutting down the reactor first?

Second, this infection highlights the importance of general nuclear plant cybersecurity. Davis-Besse was infected because of a T1 connection that bypassed the plant's firewall. Your response indicates that the NRC alerted FirstEnergy (and other NRC licensees) to this potential vulnerability in February 2002, and Information Notice 2003-14 notes that First Energy's Information Technology personnel claimed to have "addressed" the issue. But the T1 line reportedly remained in place because plant computer engineers were never informed of the vulnerability or the decision to address it.

- When the NRC alerted licensees to the vulnerability exploited by the Slammer worm, did it also require by Order or regulation that the licensees address the vulnerability? If not, why not?
- Has the Davis-Besse licensee been cited or subjected to any penalty for their Information Technology personnel falsely claiming to have addressed the T1 issue, when in fact the company's relevant computer engineers were never

informed of the situation and took no action to ameliorate it? If so, what penalty has been imposed? If not, why not?

- In the future, does the NRC plan to issue Orders or regulations to require corrective action by licensees as soon as it becomes aware of cyber vulnerabilities such as the one exploited by the Slammer worm? If not, why not?
- Will the NRC now require by Order or regulation that all network connections to nuclear plants go through a firewall? If not, why not?
- Has the NRC changed the standards by which it judges whether a licensee has sufficiently addressed an Order or regulation relating to cyber security in order to confirm that action has actually been taken?
- Will the NRC in the future confirm that plant computer engineers ultimately enact orders, rather than rely on assurances of IT personnel?

Even with the backdoor T1 line in place, the infection apparently could have been avoided if plant computer engineers had installed the Microsoft SQL Server 2000 patch released on July 10, 2002 – six months before the infection.²

- Will the NRC now require by Order or regulation that licensees install computer security patches within a reasonable time of when they become available? If not, why not?
- Will the NRC now require its regional offices and resident inspectors to confirm that action has been taken by a licensee to install computer security patches within a reasonable time after the NRC has alerted licensees or ordered action? If not, why not?

You explain in your response that the NRC has conducted pilot studies of cybersecurity at four of the nation's 104 nuclear power plants. These studies included efforts to penetrate the systems and identified "common vulnerabilities relating to the network architecture".

- Which four plants were the subjects of these studies? Why were they chosen?
- What specific cyber vulnerabilities (if any) were found at these plants, and what was done to fix them?
- Did these studies include combined cyber and physical attack simulations? If so, what did they conclude regarding such attacks? If not, why not?
- In the past five years, what other nuclear plants have been either infected with a computer virus or subject to computer hacking attempts? In each instance, what action(s) were taken by the Commission and by the licensee in response to the virus/hacker attack?
- Does the NRC intend to study cyber security at any facilities beyond the four covered by the pilot studies? If so, which plants will it study and when? If not, why is it not studying cyber security at the other 100 U.S. nuclear plants?

² See <http://www.microsoft.com/sql/downloads/>.

Please provide me with a copy of the pilot studies mentioned in your letter as soon as they are completed. Please also provide me with copies of all orders, advisories and regulations that are issued as a consequence of these studies.

You also report that the NRC is working with the nuclear industry's trade association, the Nuclear Energy Institute (NEI) to develop cybersecurity guidelines.

- In addition to consulting with the trade association for the nuclear utility industry, is the NRC consulting with governmental and private, non-NEI cybersecurity experts in developing these guidelines? If so, with whom is the NRC consulting? If not, why is the NRC not consulting with other parties?
- Specifically, is the NRC consulting with the Department of Homeland Security's National Cyber Security Division³, the National Institute of Standards and Technology's Computer Security Resource Center⁴, or the internationally recognized CERT Coordination Center at Carnegie Mellon University⁵ in developing these guidelines? If not, why not?
- Is the NRC holding public hearings or soliciting public comment about these guidelines? If so, please provide details. If not, why not?
- Will the cybersecurity guidelines be binding on licensees by Order or regulation? What will be the penalties for non-compliance?
- If the guidelines are not binding, how will the NRC ensure that the nation's nuclear plants are secure against cyber attacks?
- When will these guidelines be sent to licensees?

Please send me the cybersecurity guidelines as soon as they have been finalized.

Third, I am still trying to ascertain whether cyber attacks or computer viruses may have been involved with the August 14, 2003 blackout that paralyzed much of the Northeast and Midwest. You state that the NRC has "no information" that the blackout was caused by the Blaster worm or other cybersecurity flaw. However, the transcript of the conversation between operators at the Midwest ISO control center during the blackout specifically mentions computer troubles. For instance, while trying to figure out which lines were functional, an operator at FirstEnergy states "We have no clue. Our computer is giving us fits, too, and we don't know the status of some of the stuff around us."⁶ Later the same operator says "We are trying to [figure out what is going on]. Our computer is not happy and is not cooperating either."⁷

- Is the NRC investigating the possible role of the Blaster worm specifically and cybersecurity generally in the August 14, 2003 blackout? If so, what role is the NRC playing in this investigation and what has it learned? If not, why not?

³ See <http://www.dhs.gov/dhspublic/display?theme=52>.

⁴ See <http://csrc.nist.gov/>.

⁵ See <http://www.cert.org/>.

⁶ See <http://energycommerce.house.gov/108/hearings/09032003Hearing1061/d.pdf>, page 32, line 20.

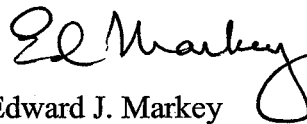
⁷ See <http://energycommerce.house.gov/108/hearings/09032003Hearing1061/d.pdf>, page 33, line 17.

Finally, you state that FirstEnergy was not in violation of NRC's requirements when the Davis-Besse plant was infected, but that the NRC has issued a notice to licensees regarding this incident.

- Why did the NRC take over seven months from the date of the Davis-Besse infection (January 25, 2003) to issue Information Notice 2003-14 (August 29, 2003)? Had I not written you on this subject, would this information notice have ever been sent?
- If the Slammer worm didn't affect safety at the Davis-Besse plant and there was no violation, why did the NRC send out Information Notice 2003-14 at all?
- If allowing a computer virus to penetrate backdoor on a T1 line, bypass a computer firewall at a nuclear facility, and infect systems used for monitoring nuclear power plant operations is **not** a violation of NRC regulatory requirements, doesn't that suggest these requirements are inadequate and may need revision?

I look forward to your reply. The NRC has a serious responsibility to keep our nation's nuclear plants safe from harm: physical, cyber and otherwise. I appreciate your efforts on nuclear cybersecurity to date and I hope you will continue to pay close attention to this critical issue. If you have any questions or concerns, please have your staff contact Dr. Colin McCormick or Mr. Jeff Duncan of my staff at 202-225-2836.

Sincerely,

A handwritten signature in dark ink, appearing to read "Ed Markey", with a stylized flourish at the end.

Edward J. Markey
Member of Congress